Backup, Restore & Disaster Recovery

California Business Connect Project

California Secretary of State

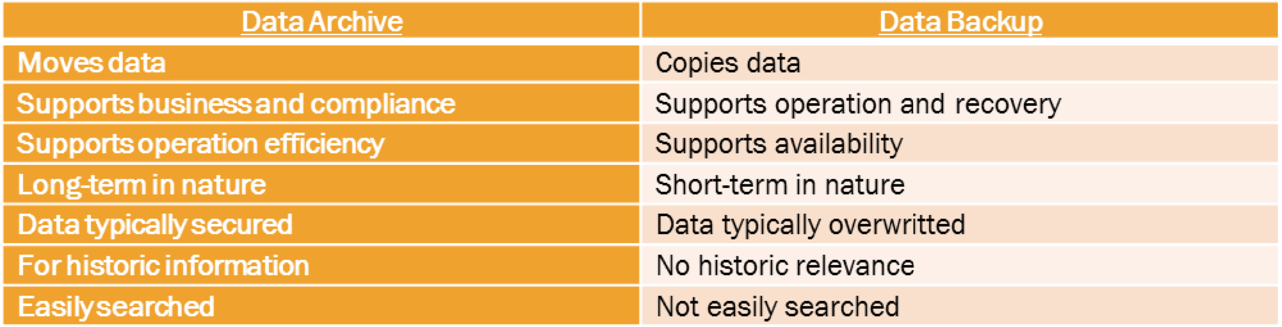
backup

- As it relates to Backup and Recovery, the copying, preservation and storage of computer data, operating systems, application code and configuration of all components of the California Business Connect Solution so it may be used to restore the original after a data loss event, whether by data deletion, corruption or other causes. Preservation encompasses the assurance of the integrity of the original data including the data, and metadata of the file, configuration or object.

Backup v. archive

Backing up involves making an image of active production data at regular intervals to protect against disaster, media failure, and human error.

Archiving stores static data for the indefinite future, with the goals of long-term data retention and compliance with legal and regulatory requirements.



Data Archive	Data Backup
Moves data	Copies data
Supports business and compliance	Supports operation and recovery
Supports operation efficiency	Supports availability
Long-term in nature	Short-term in nature
Data typically secured	Data typically overwritted
For historic information	No historic relevance
Easily searched	Not easily searched

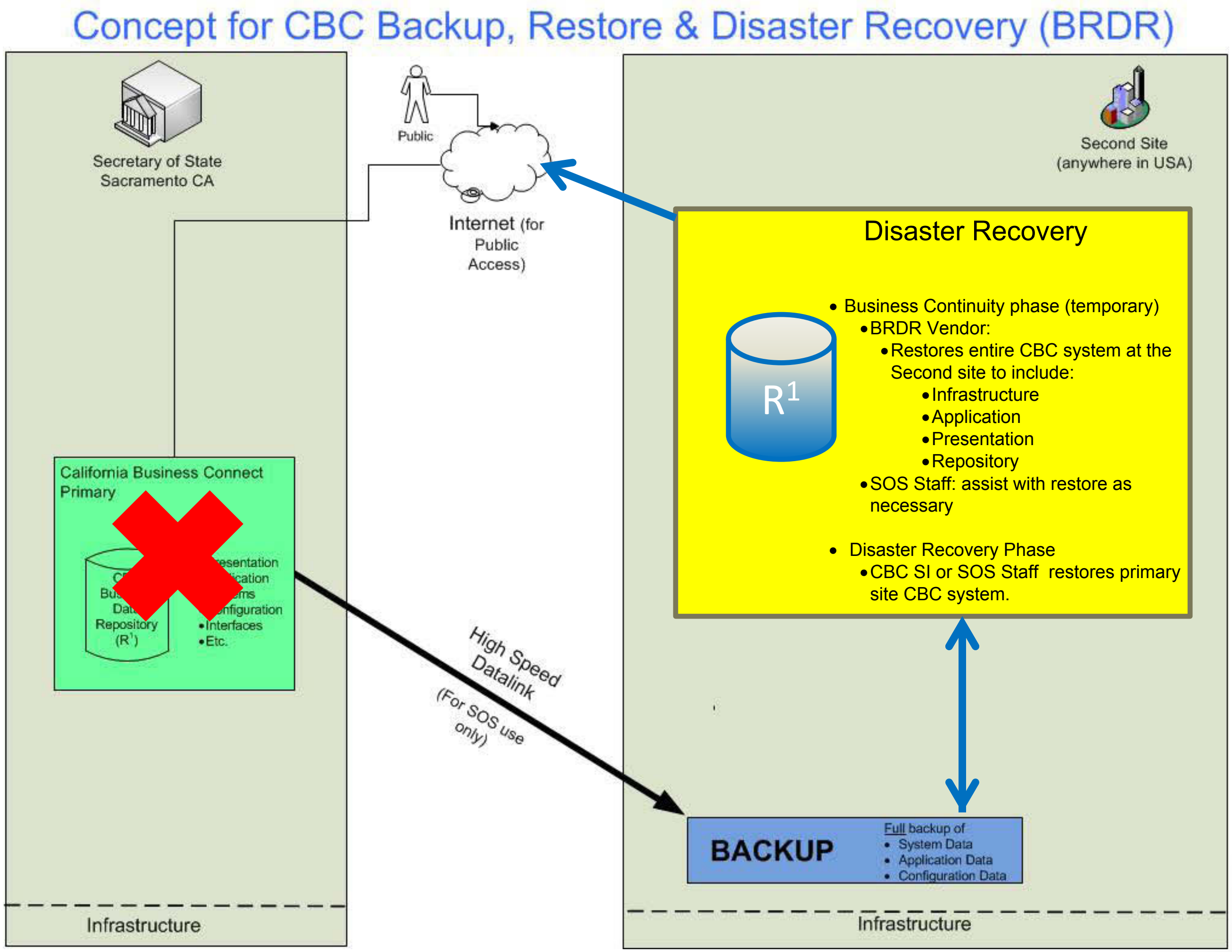
Restore

- The retrieving of previously copied and preserved computer data to original or alternate locations for recovery of a system or state at a given point in time.

Disaster recovery

- Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery is a subset of business continuity. While business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events, disaster recovery focuses on the IT or technology systems that support business functions.

BRDR – when disaster occurs



Concept for CBC Backup, Restore & Disaster Recovery (BRDR)

Secretary of State
Sacramento CA

Public

Internet (for Public Access)

Second Site
(anywhere in USA)

California Business Connect Primary

C
Bu
Dat
Repository
(R1)

esentation
ication
ems
nfiguration
- Interfaces
- Etc.

High Speed Datalink

(For SOS use only)

Disaster Recovery

R1

- Business Continuity phase (temporary)
  - BRDR Vendor:
    - Restores entire CBC system at the Second site to include:
      - Infrastructure
      - Application
      - Presentation
      - Repository
  - SOS Staff: assist with restore as necessary
- Disaster Recovery Phase
  - CBC SI or SOS Staff restores primary site CBC system.

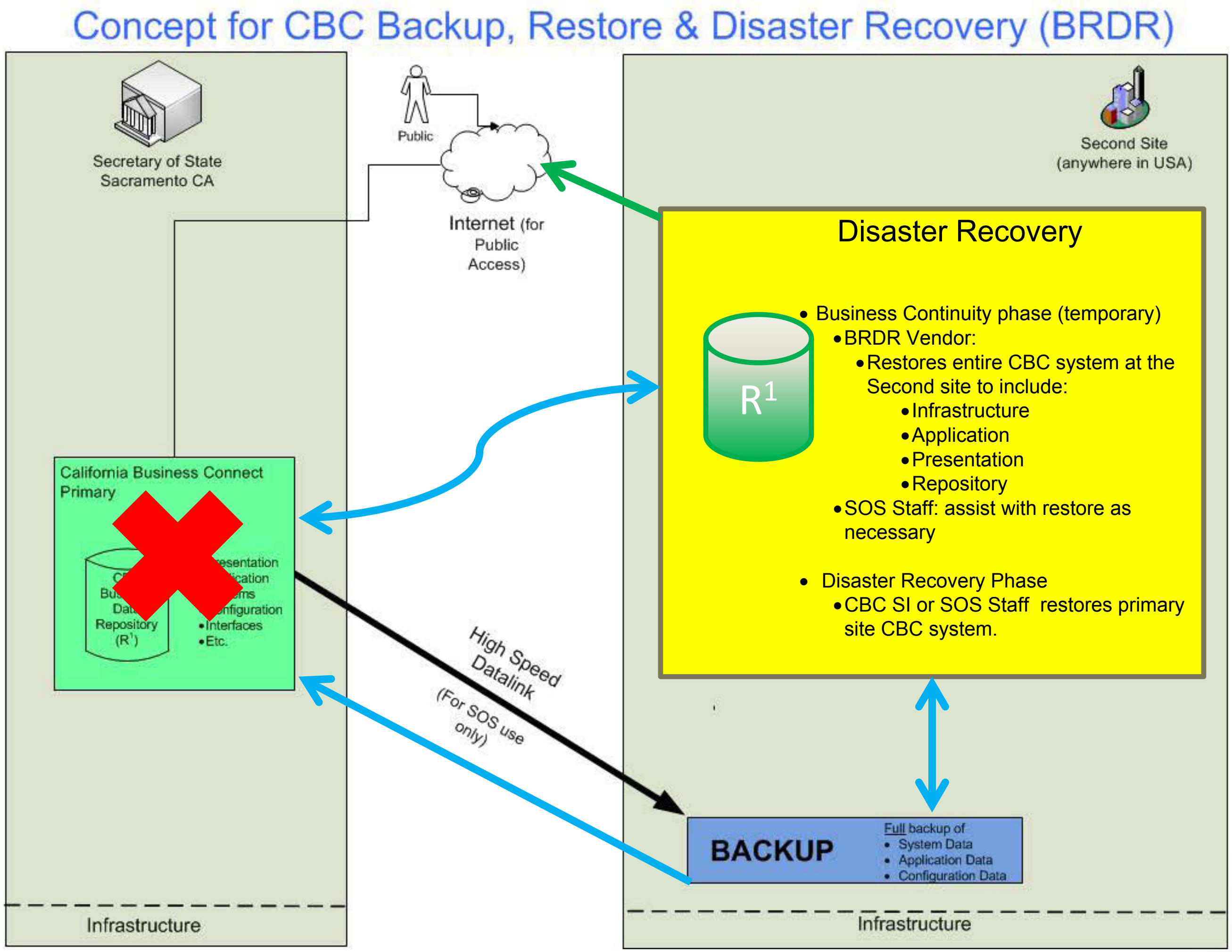
BACKUP

Full backup of
- System Data
- Application Data
- Configuration Data

Infrastructure

Infrastructure

BRDR – restoring from DR



Concept for CBC Backup, Restore & Disaster Recovery (BRDR)

Disaster Recovery

- Business Continuity phase (temporary)
  - BRDR Vendor:
    - Restores entire CBC system at the Second site to include:
      - Infrastructure
      - Application
      - Presentation
      - Repository
  - SOS Staff: assist with restore as necessary
- Disaster Recovery Phase
  - CBC SI or SOS Staff restores primary site CBC system.

BACKUP

Full backup of
- System Data
- Application Data
- Configuration Data

Backup-Restore-Disaster Recovery

What	**Definition**	**Responsible Entity Prior to Full System Acceptance**	**Responsible Entity at After Full System Acceptance**
Backup (B):	The copying, preservation and archiving of computer data so it may be used to restore the original after a data loss event, whether by data deletion, corruption or other causes. Preservation encompasses the assurance of the integrity of the original data including the data, and metadata of the file, configuration or object.	SI Vendor is solely responsible for all backup of CBC Solution data, configuration, systems, files, etc.	SI Vendor is responsible for: 1. Providing SOS estimated volume of data necessary to backup the CBC Solution. 2. The integration of the backup client or system into the CBC Solution. 3. The configuration, scheduling, execution and verification of backing-up the data. 4. Testing backup to ensure operational performance and integrity
			SOS is responsible for: 1. Providing a location to store the backup files.. 2. Providing conduit (network connectivity) to the backup location. 3. Oversight of backup operations.
			BRDR is responsible for: 1. Providing necessary access, space and platform performance for backup data.

What	**Definition**	**Responsible Entity Prior to Full System Acceptance**	**Responsible Entity at After Full System Acceptance**
Restore (R):	The retrieving of previously copied and preserved computer data to original or alternate locations for recovery of a system or state at a given point in time. *(note: this is not the same as the restore/restoration process as defined in the CBC Glossary. The Glossary term refers to a program functionality area.)*	SI Vendor is solely responsible for all restoration of CBC Solution data, configuration, systems, files, etc.	SI Vendor is responsible for: 1. The configuration, scheduling, execution and verification of the restoration of the data. 2. Retrieval of files, configuration and data from the backup system. 3. Restoring the CBC Solution to operational and error-free status. 4. Testing restore to ensure operational performance and integrity
			SOS is responsible for: 1. Providing a location to store the backup files. 2. Providing conduit (network connectivity) from the backup location. 3. Oversight of restoration operations
			BRDR is responsible for: 1. Providing necessary access, space and platform performance for restoration of data.

What	**Definition**	**Responsible Entity Prior to Full System Acceptance**	**Responsible Entity at After Full System Acceptance**

Disaster Recovery (DR):
Business Continuity (BC):
	Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.
	Disaster recovery is a subset of business continuity. While business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events, disaster recovery focuses on the IT or technology systems that support business functions.
	The California CIO defines all recovery planning under the definition of Operational Recovery Planning in SAM section 5355.2.
	The continuation of technology infrastructure vital to an organization after a natural or human-induced event that causes service disruption. Maintaining some or all aspects of a business functioning in the midst of disruptive events. Disaster recovery focuses on the IT or technology systems that support business functions.
		SOS responsible for DR of all agency operations and services.
		No DR for SI Vendor CBC Solution prior to full system acceptance.
			SI Vendor is responsible for:
			1. Maintaining proper, detailed and up-to-date documentation for the CBC Solution.
			2. Restoring Primary CBC Solution site to operational and error-free status following the declaration of a disaster.
			3. Testing the restoration of the CBC Solution from a DR scenario annually.

			SOS is responsible for: 1. Declaration of a disaster and activation the Disaster Recovery Site. 2. Maintaining necessary infrastructure at the BRDR site. 3. Providing alternate work site if primary is unavailable, including space, power, environmental controls, equipment and connectivity. 4. Sponsor (pay for) and coordinate necessary connectivity to required functional partners. 5. Planning, coordinating and executing a test of the DR operations annually.
			BRDR is responsible for: 1. Providing necessary platform operations for recovering the CBC Solution to temporary operational status. 2. Providing interim CBC Solution functionality during declared disaster according to SLA with SOS. 3. Providing storage of backup data and repository during the period of disaster operations. 4. Providing necessary connectivity to required functional partners.